Manuscript submitted to
AIMS' Journals
Volume **X**, Number **0X**, XX **200X**

Website: http://AIMsciences.org
pp. **X–XX**

CONSTRUCTIVE CONJUGATE CODES FOR QUANTUM ERROR CORRECTION AND CRYPTOGRAPHY

MITSURU HAMADA

Quantum Information Science Research Center
Tamagawa University Research Institute
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan
PRESTO, Japan Science and Technology Agency
4-1-8 Honcho, Kawaguchi, Saitama, Japan

(Communicated by an editor)

Abstract. A conjugate code pair is defined as a pair of linear codes either of which contains the dual of the other. A conjugate code pair represents the essential structure of the corresponding Calderbank-Shor-Steane (CSS) quantum error-correcting code. It is known that conjugate code pairs are applicable to quantum cryptography. In this work, a polynomial construction of conjugate code pairs is presented. The constructed pairs achieve the highest known achievable rate on additive channels, and are decodable with algorithms of polynomial complexity.

1. Introduction.

Algebraic coding has proved useful not only on 'classical' channels, already in practical use, but also on 'quantum' channels, i.e., on those that behave in quantum theoretical manners. In particular, problems of secure information transmission through quantum channels in the presence of eavesdroppers have attracted great attention [1, 2, 3] since a quantum key distribution protocol was proved secure without resort to unproven computational assumptions [2].

On the one hand, there is a large literature of physics on design and analysis of physical layers of such systems. On the other hand, the design issue of codes in this context has left much room for investigation whereas the influential work [3] on quantum key distribution suggests that the key technique of such cryptographic systems is algebraic coding.

Codes that can be used in cryptographic protocols, as well as for quantum error correction, have been treated in [4, 5, 6, 7], and the present work is a continuation. The codes of our concern here are essentially Calderbank-Shor-Steane (CSS) quantum codes as in [3, 4, 6, 7]. For CSS codes, however, we use an almost synonym *conjugate code pairs*, which would represent the essence of CSS quantum codes. A conjugate code pair is defined as a pair of linear codes either of which contains the dual of the other.

2000 *Mathematics Subject Classification.* Primary:94B70, 81P68 ; Secondary: 94B05, 11T71, 94A24.

Key words and phrases. Decoding error probability, concatenation, conjugate code pairs, constructible, quotient codes.

This work was presented in part at 2006 IEEE Information Theory Workshop, Chengdu, China, Oct., 2006.

This work presents an 'explicit', or more precisely, polynomial construction of conjugate code pairs. The constructed codes fall in the class of concatenated conjugate codes recently proposed by the present author [7]. These are conjugate code pairs dually equipped with the structure of concatenated codes [8].

Recall there exist two major design criteria for error-correcting codes, or simply codes: (i) decoding error probability of a code, and (ii) minimum distance of a code. Whereas (ii) is adopted as a measure of the goodness of a code in [9] to show that the codes in [7] are better than those known, we adopt (i) in this paper. This would be legitimate in the context of Shannon theory.

The remaining part of the paper is outlined here. After preliminaries are given in Section 2, the problem to be treated is described in Section 3. In Section 4, a 'balanced' ensemble of conjugate codes is given, and then, it is argued that a good code exists in a balanced ensemble of codes. In fact, a large portion of a balanced ensemble is made of good codes. This fact is used in a polynomial construction of codes in Section 7 while Sections 5 and 6 are devoted to explaining needed basic notions, i.e., quotient codes and concatenated conjugate codes, respectively. We conclude with a summary and remarks in Section 8.

2. **Preliminaries.** To focus on the design issue of codes, we begin directly with treating codes over a finite field, and evaluate the performance of codes in terms of classical probabilities. How the evaluation implies the reliability and security of the corresponding quantum codes or cryptographic protocols can be found in [3, 4, 6].

We fix our notation, and recall some useful tools here. As usual, $\lfloor a \rfloor$ denotes the largest integer a' with $a' \leq a$, and $\lceil a \rceil = -\lfloor -a \rfloor$. An $[n, k]$ linear (error-correcting) code over a finite field $\mathbb{F}_q$, the finite field of q elements, is a k-dimensional subspace of $\mathbb{F}_q^n$. The dual of a linear code $C \subseteq \mathbb{F}_q^n$ is $\{y \in \mathbb{F}_q^n \mid \forall x \in C,\ x \cdot y = 0\}$ and denoted by $C^\perp$, where $\cdot$ denotes the ordinary (Euclidean) inner product. The method of *types* in information theory [10, 11] is a standard tool for elementary and combinatorial analysis on probabilities. Geometric Goppa codes (algebraic geometry codes) will be used in Section 7, while the same achievable rate can be obtained with the more elementary Reed-Solomon (RS) codes with a slower speed of convergence of error probability to zero [12]. Whereas geometric Goppa codes were originally described in the language of algebraic geometry, these can, more directly, be described in the language of the function fields [13], which we will use. The notion of polynomial constructibility is well established in coding theory [14, p. 80], [15, p. 317]: A sequence of codes $\{C_\nu\}$ of growing length is said to be polynomially constructible or *polynomial* if their encoders or generator matrices of C_ν are constructible with polynomial complexity in their code-length. Similarly, our conjugate codes to be presented are polynomial in that generator matrices of them can be produced with polynomial complexity as the conjugate codes in [9].

3. **Theme.** Consider a pair of linear codes (C_1, C_2) satisfying

$$C_2^\perp \subseteq C_1, \tag{1}$$

which condition is equivalent to $C_1^\perp \subseteq C_2$. The following question arises from an issue on quantum cryptography [3] (also explained in [6, 5]): How good both C_1 and C_2 can be under the constraint (1)?

We have named a pair (C_1, C_2) with (1) a conjugate (complementary) code pair, or more loosely, conjugate codes. We remark that a CSS quantum code is specified by a conjugate code pair (C_1, C_2) (put $\mathcal{C}_1 = C_1, \mathcal{C}_2 = C_2^\perp$ in [16]; C_1 corrects bit

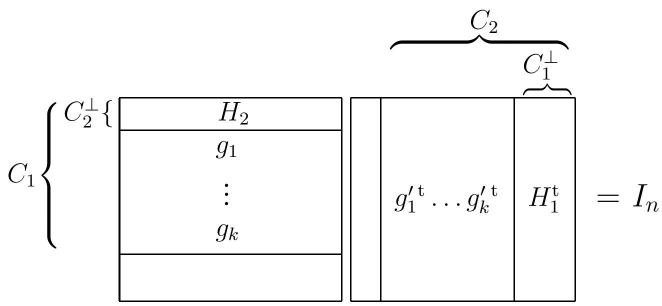

FIGURE 1. A basic structure of an $[[n, k]]$ conjugate code pair.

flip errors and C_2 corrects phase errors). CSS codes form a class of algebraic quantum error-correcting codes called symplectic or stabilizer codes ([17] and references therein).

4. **Good Codes in a Balanced Ensemble.** We can find good codes in an ensemble if the ensemble is balanced in the following sense (e.g., [5]). Suppose A is an ensemble of subsets of $\mathbb{F}_q^n$. If there exists a constant V such that $|\{C \in \mathsf{A} \mid x \in C\}| = V$ for any word $x \in \mathbb{F}_q^n \setminus \{0_n\}$, where $0_n \in \mathbb{F}_q^n$ is the zero vector, the ensemble A is said to be *balanced*.

We will construct a relatively small ensemble B of conjugate code pairs (C_1, C_2) such that both $\{C_1 \mid (C_1, C_2) \in \mathsf{B}\}$ and $\{C_2 \mid (C_1, C_2) \in \mathsf{B}\}$ are balanced. Let T be the companion matrix [18] (the definition can also be found in [7]), or its transpose, of a primitive polynomial of degree n over $\mathbb{F}_q$. Given an $n \times n$ matrix M, let $M|^m$ (respectively, $M|_m$) denote the $m \times n$ submatrix of M that consists of the first (respectively, last) m rows of M. We put $C_1^{(i)} = \{xT^i|^{k_1} \mid x \in \mathbb{F}_q^{k_1}\}$ and $C_2^{(i)} = \{x(T^{-i})^{\mathrm{t}}|_{k_2} \mid x \in \mathbb{F}_q^{k_2}\}$ for $i = 0, \dots, q^n - 2$, where M^{t} denotes the transpose of M. Then, setting

$$\mathsf{B} = \mathsf{B}(T) = \{(C_1^{(i)}, C_2^{(i)}) \mid i = 0, \dots, q^n - 2\}, \tag{2}$$

we have the next lemma.

Lemma 4.1. *For integers k_1, k_2 with $0 \le n - k_2 \le k_1 \le n$ and $\mathsf{B} = \mathsf{B}(T)$ constructed as above, any $(C_1, C_2) \in \mathsf{B}$ is a conjugate code pair, and both $\{C_1 \mid (C_1, C_2) \in \mathsf{B}\}$ and $\{C_2 \mid (C_1, C_2) \in \mathsf{B}\}$ are balanced.*

Remark. The matrix T may, more generally, be an $n \times n$ invertible matrix over $\mathbb{F}_q$ of the following properties. (i) The set $\{O_n, I_n, T, \dots, T^{q^n-2}\}$ is closed under the addition and multiplication, where O_n and I_n denote the zero matrix and identity matrix, respectively. (ii) The matrix T has multiplicative order $q^n - 1$.

Proof of Lemma 4.1. The condition (1) is fulfilled since $T^i T^{-i} = I_n$ implies that the $C_2^{(i)\perp}$ is spanned by the first $n - k_2$ rows of T^i. (Consider the situation where the matrix equation in Figure 1 is $T^i T^{-i} = I_n$. The picture was drawn for a generic conjugate code pair in [7].)

We can write $C_1^{(i)} = \{yT^i \mid y \in \mathbb{F}_q^n, \operatorname{\mathsf{supp}} y \subseteq [1, k_1]_{\mathbb{Z}}\}$, where $\operatorname{\mathsf{supp}}(y_1, \dots, y_n) = \{i \mid y_i \ne 0\}$, and $[i, j]_{\mathbb{Z}} = \{i, i+1, \dots, j\}$ for integers $i \le j$. Imagine we list up all codewords in $C_1^{(i)}$ allowing duplication. Specifically, we list up all yT^i as y and i vary over the range $\{y \mid y \in \mathbb{F}_q^n, \operatorname{\mathsf{supp}} y \subseteq [1, k_1]_{\mathbb{Z}}\}$ and over $[0, q^n - 2]_{\mathbb{Z}}$, respectively.

With $y \in \mathbb{F}_q^n \setminus \{0\}$ fixed, yT^i, $i \in [0, q^{n-2}]_{\mathbb{Z}}$, are all distinct since $T^i \neq T^j$ implies $yT^i - yT^j = yT^l$ for some l and yT^l is not zero. Hence, any nonzero fixed word in $\mathbb{F}_q^n$ appears exactly $q^{k_1} - 1$ times in listing yT^i as above. Namely, the ensemble $\{C_1 \mid (C_1, C_2) \in \mathsf{B}\}$ is balanced. Using $(T^{-i})^{\mathrm{t}}$ in place of T^i, we see the ensemble of C_2 is also balanced, completing the proof. □

To proceed, we need some notation. We denote the type of $x \in \mathbb{F}_q^n$ by P_x [10, 11]. This means that the number of appearances of $u \in \mathbb{F}_q$ in $x \in \mathbb{F}_q^n$ is $n\mathsf{P}_x(u)$. The set of all types of sequences in $\mathbb{F}_q^n$ is denoted by $\mathcal{P}_n(\mathbb{F}_q)$. Given a set $C \subseteq \mathbb{F}_q^n$, we put $M_Q(C) = |\{y \in C \mid \mathsf{P}_y = Q\}|$ for types $Q \in \mathcal{P}_n(\mathbb{F}_q)$. The list of numbers $(M_Q(C))_{Q \in \mathcal{P}_n(\mathbb{F}_q)}$ may be called the P-spectrum (or simply, spectrum) of C. For a type Q, we put $\mathcal{T}_Q^n = \{y \in \mathbb{F}_q^n \mid \mathsf{P}_y = Q\}$. We denote by $\mathcal{P}(\mathbb{F}_q)$ the set of all probability distributions on $\mathbb{F}_q$.

We use the next proposition, which relates the spectrum of a code with its decoding error probability when it is used on the additive memoryless channel characterized by a probability distribution W on $\mathbb{F}_q$, which changes an input $x \in \mathbb{F}_q$ into y with probability $W(y - x)$. This kind of error bound has appeared in [19] while the present form is from [5, Theorem 4].

Proposition 1. *Suppose we have an $[n, \kappa]$ linear code C over $\mathbb{F}_q$ such that*

$$M_Q(C \setminus \{0_n\}) \leq a_n q^{\kappa - n} |\mathcal{T}_Q^n|, \quad Q \in \mathcal{P}_n(\mathbb{F}_q)$$

where 0_n is the zero vector in $\mathbb{F}_q^n$. Then, if $a_n \geq 1$, its decoding error probability with the minimum entropy syndrome decoding is upper-bounded by

$$a_n |\mathcal{P}_n(\mathbb{F}_q)|^2 d^{-nE_{\mathrm{r}}(W,r)}$$

for any additive channel W of input-output alphabet $\mathbb{F}_q$, where $r = \kappa/n$ and $E_{\mathrm{r}}(W, r)$ is the random coding exponent of W defined by

$$E_{\mathrm{r}}(W, r) = \min_{Q \in \mathcal{P}(\mathbb{F}_q)} [D(Q||W) + |1 - r - H(Q)|^+].$$

Here, D and H denote the relative entropy and entropy, respectively, and $|x|^+ =$ $\max\{0, x\}$.

In the simplest case where $q = 2$, the premise of the above proposition reads 'the spectrum of C is approximated by the binomial coefficients $|\mathcal{T}_Q^n|$ up to normalization.' By a straightforward argument using Markov's inequality, we have the next lemma and estimate for the number of bad codes in (4) below (a proof can be found in [12]).

Lemma 4.2. *We have*

$$M_Q(C_j \setminus \{0_n\}) \leq 2(|\mathcal{P}_n(\mathbb{F}_q)| - 1) q^{k_j - n} |\mathcal{T}_Q^n|, \quad Q \in \mathcal{P}_n(\mathbb{F}_q),\ j = 1, 2$$

for some conjugate code pair $(C_1, C_2) \in \mathsf{B}$.

The codes C_1 and C_2 in Lemma 4.2 both attain the random coding exponent by Proposition 1. Thus, we have a conjugate code pair (C_1, C_2) such that both the $[n, k_1]$ code C_1 and the $[n, k_2]$ code C_2, used on W_1 and on W_2, have asymptotically vanishing decoding error probabilities, as far as the asymptotic rates are below $1 - H(W_1)$ and $1 - H(W_2)$, respectively.

In fact, a large portion of a balanced ensemble is made of good codes. Specifically, let us say an $[n, k_j]$ code $C_j^{(i)}$ is A-good if

$$M_Q(C_j^{(i)} \setminus \{0_n\}) \leq (|\mathcal{P}_n(\mathbb{F}_q)| - 1) q^{-n(1 - r_j)} A \tag{3}$$

for all $Q \in \mathcal{P}_n(\mathbb{F}_q)$, where $r_j = k_j/n$. Then, by Markov's inequality, the number of codes that are not $q^{\varepsilon n}$-good in $\{C_j \mid (C_1, C_2) \in \mathsf{B}\}$ is at most

$$z = \lfloor N q^{-\varepsilon n} \rfloor. \tag{4}$$

For $q^{\varepsilon n}$-good codes $C_j^{(i)}$, the decoding error probability is upper-bounded by

$$P_j = a_n q^{-n[E_{\mathrm{r}}(W, r_j) - \varepsilon]}, \quad j = 1, 2, \tag{5}$$

where $a_n = |\mathcal{P}_n(\mathbb{F}_q)|^3$ is at most polynomial in n, owing to Proposition 1.

5. **Quotient Codes and a Closer Look at Theme.** We have been seeking a pair (C_1, C_2) with (1) such that both C_1 and C_2 are good. However, this requirement can be weakened slightly. In fact, we are interested in a pair (C_1, C_2) such that both quotient codes $C_1/C_2^{\perp}$ and $C_2/C_1^{\perp}$ are good in the context of cryptography [3, 6, 5] as well as in that of quantum error correction.

A *quotient code* C/B means an additive quotient group C/B, and can be used for transmission of information in the following way. We encode a message into a member of $c \in C/B$, which has the form $x + B$, and then transmit a randomly chosen word in c. Clearly, if C is J-correcting in the ordinary sense, C/B is $(J + B)$-correcting. For the purpose of transmission of information only, dividing the code C by B does not seem meaningful, but this scheme has proved useful for transmission of secret information in the presence of eavesdroppers. The role of B may be understood as a kind of scrambler. This scenario is due to [20] while the term quotient code was coined in [5].

As mathematical objects, the conjugate code pairs (C_1, C_2) and the quotient codes C/B are obviously in one-to-one correspondence: $(C_1, C_2) \leftrightarrow C_1/C_2^{\perp}$, or $(C_1, C_2) \leftrightarrow C_2/C_1^{\perp}$. We mean by an $[[n, k]]$ conjugate code pair over $\mathbb{F}_q$ a pair (C_1, C_2) consisting of an $[n, k_1]$ linear code C_1 and an $[n, k_2]$ linear code C_2 over $\mathbb{F}_q$ satisfying (1) and

$$k = k_1 + k_2 - n. \tag{6}$$

The number k/n is called the *(information) rate* of the conjugate code pair (C_1, C_2), and equals that of quotient code $C_1/C_2^{\perp}$, that of $C_2/C_1^{\perp}$, and that of the corresponding CSS quantum code.

The goal is to find a conjugate code pair (C_1, C_2) such that both $C_1/C_2^{\perp}$ and $C_2/C_1^{\perp}$ are good on either of the criteria mentioned in Section 1. If the linear codes C_1 and C_2 are both good, so are $C_1/C_2^{\perp}$ and $C_2/C_1^{\perp}$. Hence, a conjugate code pair (C_1, C_2) with good C_1 and C_2 is also desirable.

6. **Concatenated Conjugate Codes.** We recall how the *concatenation* (L_1, L_2) of inner $[[n^{(i)}, k]]$ conjugate code pairs $(C_1^{(i)}, C_2^{(i)})$ over $\mathbb{F}_q$, $i = 1, \dots, N$, and an outer $[[N, K]]$ conjugate code pair (D_1, D_2) over $\mathbb{F}_{q^k}$ was obtained in [7] (the result also appeared in [12]) retaining the notation of [7, 12]. For $j = 1, 2$, let $\pi_j^{(i)}$ be a one-to-one $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^k}$ onto a set of coset representatives of $C_j^{(i)}/C_{\overline{j}}^{(i)\perp}$, where $\overline{1} = 2$ and $\overline{2} = 1$, and $\pi_j(x)$ denote the juxtaposition $\pi_j^{(1)}(x_1) \cdots \pi_j^{(N)}(x_N) \in \mathbb{F}_q^{\sum_i n^{(i)}}$ of $\pi_j^{(i)}(x_i)$, $i \in \{1, \dots, N\}$, for $x = (x_1, \dots, x_N) \in \mathbb{F}_{q^k}^N$. Then, $L_j = \pi_j(D_j) + \overline{C_{\overline{j}}^{\perp}}$, where $\overline{C_{\overline{j}}^{\perp}} = \bigoplus_{i=1}^N C_{\overline{j}}^{(i)\perp}$.

For (L_1, L_2) to satisfy the constraint $L_2^{\perp} \subseteq L_1$, we need a certain condition on π_1 and π_2. In fact, by a proper choice of π_1 and π_2 based on dual bases of $\mathbb{F}_{q^k}$ and the structure of conjugate codes as depicted in Figure 1, we have the next theorem.

Theorem 6.1. [7]

$$[\pi_1(D_2^{\perp}) + \overline{C_2^{\perp}}]^{\perp} = \pi_2(D_2) + \overline{C_1^{\perp}}, \quad [\pi_2(D_1^{\perp}) + \overline{C_1^{\perp}}]^{\perp} = \pi_1(D_1) + \overline{C_2^{\perp}}.$$

7. **Polynomial Construction of Codes.** Using almost all codes in $\mathsf{B}(T)$ as inner codes, we will construct the desired codes. The point of the argument below is that, by Markov's inequality, all but a negligible number of the inner codes are good (Section 4), so that the overall performance is also good [21].

Theorem 7.1. *Let $R_{\rm o}$ be a number that can be written as $R_{\rm o} = (r_1 + r_2 - 1)(R_1 + R_2 - 1)$ with some $r_1, r_2, R_1, R_2 \in (0, 1]$, $r_1 + r_2 - 1 \geq 0, R_1 + R_2 - 1 \geq 0$. Then, we have a sequence of $[[N_{\rm o}, K_{\rm o}]]$ conjugate code pairs (L_1, L_2) over $\mathbb{F}_q$ such that the rate $K_{\rm o}/N_{\rm o}$ approaches $R_{\rm o}$, a parity-check matrix of L_2 and that of $L_1^{\perp}$ can be produced with algorithms of polynomial complexity, and the decoding error probability $P_{{\rm e},j}$ of $L_j/L_{\overline{j}}^{\perp}$, where $\overline{1} = 2$ and $\overline{2} = 1$, is bounded by*

$$\limsup_{N_{\rm o}\to\infty} -\frac{1}{N_{\rm o}} \log_q P_{{\rm e},j} \geq \frac{1}{2}(1 - R_j)E(W_j, r_j), \quad j = 1, 2$$

for any additive channels W_1, W_2 of input-output alphabet $\mathbb{F}_q$, where $E(W_j, r_j)$ is the random coding exponent $E_{\rm r}(W_j, r_j)$. Moreover, we have a polynomial decoding algorithm for the quotient code $L_2/L_1^{\perp}$.

Corollary 1. *Let a number $R_{\rm o} \in (0, 1]$ be given. Then, we have a sequence of conjugate code pairs (L_1, L_2) satisfying the same conditions as in the theorem except the bound on $P_{{\rm e},j}$, which is to be replaced by*

$$\limsup_{N_{\rm o}\to\infty} -\frac{1}{N_{\rm o}} \log_q P_{{\rm e},j} \geq \frac{1}{2} \sup_{r_1,r_2,R_1,R_2} \min_{l\in\{1,2\}} (1 - R_l)E(W_l, r_l), \quad j = 1, 2$$

for any additive channels W_1, W_2, where the supremum is taken over $\{(r_1, r_2, R_1, R_2) \in (0, 1]^4 \mid r_1 + r_2 - 1 \geq 0,\ R_1 + R_2 - 1 \geq 0,\ (r_1 + r_2 - 1)(R_1 + R_2 - 1) = R_{\rm o}\}$.

Remarks. The decoder for $L_2/L_1^{\perp}$, as well as the construction of $L_2/L_1^{\perp}$, is independent from the channel. The bound in the theorem is also valid for $E(W, r_{\rm c}) = \max\{E_{\rm r}(W, r_{\rm c}), E_{\rm ex}(W, r_{\rm c})\}$, where $E_{\rm ex}$ is as in [5, Theorem 4], but in this case, the decoder for $L_2/L_1^{\perp}$ would depend on the channel in general. Here, the decoding complexity should be understood as that of quotient codes as described in Section 5 or [5], not that of quantum codes.

Proof. We will construct (L_1, L_2) by concatenation retaining the notation of Section 6. We use almost all $(C_1^{(i)}, C_2^{(i)})$ in B for inner codes, where $C_j^{(i)}$ is an $[n, k_j]$ code for all i $(j = 1, 2)$. For outer codes, we use polynomially constructible geometric Goppa codes of large minimum distance. Namely, we use codes over $\mathbb{F}_{q^k}$, where $q^k = p^m$ with some p prime and m even, obtained from function fields of many rational places (places of degree one). Specifically, we use a family of function fields $F_\nu/\mathbb{F}_{q^k}$, $\nu = 1, 2, \ldots$, such that $F_\nu/\mathbb{F}_{q^k}$ has genus $g = g_{\nu,k}$ and at least $N + 1 = N_{\nu,k} + 1$ rational places, and assume they satisfy

$$\lim_{k\to\infty} \frac{g}{N} = 0 \tag{7}$$

for any ν. This is fulfilled, e.g., by the second Garcia-Stichtenoth tower of function fields [22] with $g \le q^{k\nu/2}$ and N as in (9) below. (We remark unlike typical situations where we are concerned with the limit of g/N as $\nu \to \infty$, we fix ν here in taking the limit. The level ν is to be fitted to the target rate of inner codes by (10) below.)

If we put $A = P_1 + \cdots + P_N$, where P_i are distinct rational places in $F_\nu/\mathbb{F}_{q^k}$ and G is a divisor of $F_\nu/\mathbb{F}_{q^k}$ such that $\mathsf{supp}\, G \cap \mathsf{supp}\, A = \emptyset$, we have a geometric Goppa code $C_{\mathcal{L}}(A, G)$ defined by

$$C_{\mathcal{L}}(A,G) = \{(f(P_1), \dots, f(P_N)) \mid f \in \mathcal{L}(G)\}$$

where $\mathcal{L}(G) = \{x \in F_\nu \mid (x) \ge -G\} \cup \{0\}$, and (x) denotes the (principal) divisor of x (e.g., as in [13, p. 16]). We assume both D_1 and $D_2^\perp$ are obtained in this way from the function field $F_\nu/\mathbb{F}_{q^k}$: $D_1 = C_{\mathcal{L}}(A, G_1)$ and $D_2 = C_{\mathcal{L}}(A, G_2)^\perp$. We require $G_2 \le G_1$ so that the CSS condition $D_2^\perp \subseteq D_1$ is fulfilled. We also assume $2g - 2 < \deg G_j < N$ for $j = 1, 2$. Then, the dimension of D_1 is

$$K_1 = \dim G_1 = \deg G_1 - g + 1,$$

and that of D_2 is

$$K_2 = N - \dim G_2 = N - \deg G_2 + g - 1.$$

The designed distance of D_1 is $N - \deg G_1$, and that of D_2 is $\deg G_2 - 2g + 2$.

We consider the asymptotic situation where for arbitrarily fixed $0 \le r_j^*, R_j^* \le 1$,

$$r_j \stackrel{\text{def}}{=} k_j/n \to r_j^* \quad \text{and} \quad R_j \stackrel{\text{def}}{=} K_j/N \to R_j^*, \quad j = 1, 2 \tag{8}$$

as $n, N \to \infty$, using a family of $[N, K_j]$ geometric Goppa codes that fulfills the following requirement as well as (7). Specific examples of such codes can be found in [23] for $\nu \ge 3$ (we can use the RS and Hermitian codes for $\nu = 1, 2$) or in [24]. We assume that N grows fast enough so as to be almost as large as the size of B as $k \to \infty$. Specifically, for any ν, we require

$$N = q^{k(\nu+1)/2} - z' \tag{9}$$

for some $z' = z'_{\nu,k}$ such that $z'/N \to 0$ as $k \to \infty$. By this assumption, if we set

$$\nu = \lceil 2n/k \rceil - 1 \tag{10}$$

so that $q^{k(\nu+1)/2} > q^n - 1 = |\mathsf{B}|$, we can use all but a negligible number $\le z'$ of code pairs in B as inner codes.

For decoding, we first decode the inner codes and then the outer code [7]. Recall we have (5). Then, employing a decoder that can correct $\lfloor (N - K_j)/2 \rfloor - g$ errors for the outer codes, we have the decoding error probability $P_{\mathrm{e},j}$ of $L_j/L_{\overline{j}}$ bounded by

$$\begin{aligned} P_{\mathrm{e},j} &\le \sum_{i=t-z}^{N-z} \binom{N-z}{i} P_j^i (1-P_j)^{N-z-i} \\ &\le q^{(t-z)\log_q P_j + (N-t)\log_q(1-P_j) + (N-z)h((t-z)/(N-z))} \end{aligned}$$

where z is as in (4), h is the binary entropy function, and $t = t_j = \lfloor (N - K_j)/2 \rfloor - g + 1$ (for the second inequality, see, e.g., [25, p. 446]). Taking logarithms and

dividing by $N_{\rm o} = nN$, we have

$$\begin{aligned}\frac{1}{N_{\rm o}} \log_q P_{{\rm e},j} \quad &\le \quad \frac{t-z}{N}\Big[- E(W, r_j) + \varepsilon + \frac{\log_q a_n}{n} \Big] \\ &\quad + \frac{1}{n}\Big[\frac{N-t}{N} \log_q(1-P_j) + \frac{N-z}{N} h\big((t-z)/(N-z)\big) \Big]\end{aligned}$$

for $j = 1, 2$. Hence, letting $k \to \infty$ with constraint (8) and using (7), we have

$$\limsup_{N_{\rm o}\to\infty} -\frac{1}{N_{\rm o}} \log_q P_{{\rm e},j} \ge \frac{1}{2}(1-R_j^*)[E(W, r_j^*) - \varepsilon]. \tag{11}$$

Then, since $\varepsilon > 0$ is arbitrary, noticing the overall rate is $kK/(nN) = (r_1 + r_2 - 1)(R_1 + R_2 - 1)$, we have the desired bounds in the theorem and corollary.

We have used a family of geometric Goppa codes D_1 and $D_2^\perp$ for which we have polynomial algorithms to produce generator matrices [23, 26], and parity-check matrices and generator matrices of concatenated conjugate codes are easily obtained from those of D_j [7]. In general, if the outer code D_j is decodable with polynomial complexity, so is the concatenated quotient code $L_j/L_{\overline{j}}^\perp$ [8, 7]. For our choice [23, 24], $D_2 = C_{\mathcal{L}}(A, G_2)^\perp$ is a 'one-point' code, i.e., the support of G_2 consists of one rational place, so that we have a polynomial decoding algorithm that corrects $\lfloor (N-K_2)/2 \rfloor - g$ errors (e.g., [13],[27]). The proof is complete. □

We remark that putting constraints $R_1^* = R_2^*$ and $r_1^* = r_2^*$ in (11), we have a weakened but closed form of the bound, which appeared in [12].

The highest achievable rate ($R_{\rm o}$ such that $P_{{\rm e},j} \to 0$ for both $j = 1$ and 2) resulting from Theorem 7.1 is $R_{\rm CSS} = 1 - H(W_1) - H(W_2)$ while the bound in [12] mentioned above implies the weaker achievable rate $R'_{\rm CSS} = 1 - 2\max\{H(W_1), H(W_2)\}$. The achievability of $R'_{\rm CSS}$ ($\le R_{\rm CSS}$) by non-constructive conjugate (CSS) codes had been established in [4] and by non-constructive but polynomially decodable conjugate codes in [7].

The improvement on $R'_{\rm CSS}$ is not novel. In fact, a bound on the error probability in [5, Section 10.3] implies the achievability of $R_{\rm CSS}$ by non-constructive codes, and the argument of [7] can easily be amended to establish the achievability of $R_{\rm CSS}$ using a good inner code shown to exist in [5, Section 10.3]. Lemma 4.2 says we can find good codes in an ensemble much smaller than that of [5, Section 10.3].

We remark that in the extreme case where $C_1^{(i)} = \mathbb{F}_q^n$ and $D_1 = \mathbb{F}_{q^k}^N$, the quotient code $L_2/L_1^\perp$ becomes the classical concatenated code L_2, and (11) applies even to this case.

8. **Summary and Remarks.** In this work, conjugate code pairs that are constructible with polynomial complexity were presented. The constructed pairs achieve the highest known achievable rate on additive channels. Moreover, the constructed codes, as quotient codes, allow decoding of polynomial complexity. We conclude with some remarks.

(I) A polynomial construction of asymptotically good quantum codes was first presented in [28]. This adopts the criterion of minimum distance and reflects the idea of polynomial constructions of classical algebraic codes ([14] and references therein). See [9] for attainable minimum distance of concatenated conjugate codes or quantum codes of analogous structure, and how it is related to [28]. The present work's approach is rather close to that of [21], which presented an explicit construction of capacity-achieving codes adopting the criterion of decoding error probability.

(II) Though a conjugate code pair is defined as a pair of *classical* codes, it is rephrased as a CSS quantum error-correcting code (Section 3). Theorem 7.1 implies that our codes, as polynomially constructible quantum codes, achieve the rate $R_{\mathrm{CSS}} = 1 - H(P_{\mathsf{X}}) - H(P_{\mathsf{Z}})$ for the channel that changes a quantum state ρ into $X^x Z^z \rho (X^x Z^z)^{-1}$ with probability $P_{\mathsf{XZ}}(x,z)$, $(x,z) \in (\mathbb{Z}/q\mathbb{Z})^2 = \{0,\dots,q-1\}^2$. Here, q is a prime, X and Z are unitary operators that represent unit shifts in complementary observables (e.g., they are distinct Pauli operators for $q=2$), and P_{U} denotes the distribution of a random variable U. (See, e.g., [29, 5, 6] for backgrounds.) This holds true for general quantum channels as well [29, 30].

(III) This work was motivated by an issue on quantum cryptography, or specifically, by the fact that good conjugate (CSS) codes can be used as the main ingredients of some quantum cryptographic protocols as argued in [3, 4, 6]. The security of such protocols using our codes can be evaluated along the lines of [3, 4].

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, pp. 175–179, 1984.

[2] D. Mayers, "Unconditional security in quantum cryptography," *J. Assoc. Comp. Mach.*, vol. 48, pp. 351–406, 2001.

[3] P. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, July 2000.

[4] M. Hamada, "Reliability of Calderbank-Shor-Steane codes and security of quantum key distribution," *J. Phys. A: Math. Gen.*, vol. 37, pp. 8303–8328, 2004. E-Print, quant-ph/0308029, LANL, 2003.

[5] M. Hamada, "Quotient codes and their reliability," *IPSJ Digital Courier*, vol. 1, pp. 450–460, Oct. 2005. Available at `http://www.jstage.jst.go.jp/article/ipsjdc/1/0/1_450/_article`. Also appeared in *IPSJ Journal*, vol. 46, pp. 2428–2438, no. 10, Oct., 2005.

[6] M. Hamada, "Conjugate codes and applications to cryptography," *Tamagawa University Research Review*, no. 12, pp. 19–25, Dec. 2006. E-Print, quant-ph/0610193, LANL.

[7] M. Hamada, "Concatenated conjugate codes," submitted to *IEEE Trans. Information Theory*, Aug. 2006. E-Print, quant-ph/0610194, LANL.

[8] G. D. Forney, Jr., *Concatenated Codes.* MA: MIT Press, 1966.

[9] M. Hamada, "Minimum distance of concatenated conjugate codes for cryptography and quantum error correction," submitted to *IEEE Trans. Information Theory*, Oct. 2006. E-Print, quant-ph/0610195, LANL.

[10] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems.* NY: Academic, 1981.

[11] I. Csiszár, "The method of types," *IEEE Trans. Information Theory*, vol. IT-44, pp. 2505–2523, Oct. 1998.

[12] M. Hamada, "Conjugate codes for secure and reliable information transmission," *Proceedings of IEEE Information Theory Workshop, Chengdu, China*, pp. 149–153, Oct. 2006.

[13] H. Stichtenoth, *Algebraic Function Fields and Codes.* Berlin: Springer-Verlag, 1993.

[14] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes.* MA: Kluwer, 1991.

[15] S. A. Stepanov, *Codes on Algebraic Curves.* New York: Kluwer/Plenum, 1999.

[16] A. R. Calderbank and P. W. Shor, "Good quantum error correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, 1996.

[17] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1369–1387, July 1998.

[18] R. Lidl and H. Niederreiter, *Finite Fields.* Cambridge: Cambridge University Press, 2nd ed., 1997.

[19] R. G. Gallager, *Low-density parity-check codes.* Cambridge, MA: MIT Press, 1963.

[20] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[21] P. Delsarte and P. Piret, "Algebraic construction of Shannon codes for regular channels," *IEEE Trans. Information Theory*, vol. 28, pp. 593–599, July 1982.

[22] A. Garcia and H. Stichtenoth, "On the asymptotic behaviour of some towers of function fields over finite fields," *Journal of Number Theory*, vol. 61, pp. 248–273, 1996.

[23] K. W. Shum, I. Aleshnikov, P. V. Kumar, H. Stichtenoth, and V. Deolalikar, "A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound," *IEEE Trans. Information Theory*, vol. 47, pp. 2225–2241, Sept. 2001.

[24] B.-Z. Shen, "A Justesen construction of binary concatenated codes that asymptotically meet the Zyablov bound for low rate," *IEEE Trans. Information Theory*, vol. IT-39, Jan. 1993.

[25] S. Roman, *Coding and Information Theory.* NY: Springer-Verlag, 1992.

[26] K. W. Shum, *A Low-Complexity Construction of Algebraic-Geometric Codes Better Than the Gilbert-Varshamov Bound*. Ph.D. thesis, Univ. of Southern California, 2000.

[27] T. Høholdt, J. H. van Lint, and R. Pellikaan, "Algebraic geometry codes," in *Handbook of Coding Theory,* V. S. Pless and W. C. Huffman eds., vol. I, pp. 871–961, 1998.

[28] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, "Asymptotically good quantum codes," *Phys. Rev. A*, vol. 63, pp. 032311–1–5, 2001.

[29] M. Hamada, "Notes on the fidelity of symplectic quantum error-correcting codes," *International Journal of Quantum Information*, vol. 1, no. 4, pp. 443–463, 2003. E-Print, quant-ph/0311003, LANL, 2003.

[30] M. Hamada, "Lower bounds on the quantum capacity and highest error exponent of general memoryless channels," *IEEE Trans. Information Theory*, vol. 48, pp. 2547–2557, Sept. 2002. E-Print, quant-ph/0112103, LANL, 2001.

E-mail address: `mitsuru@ieee.org`